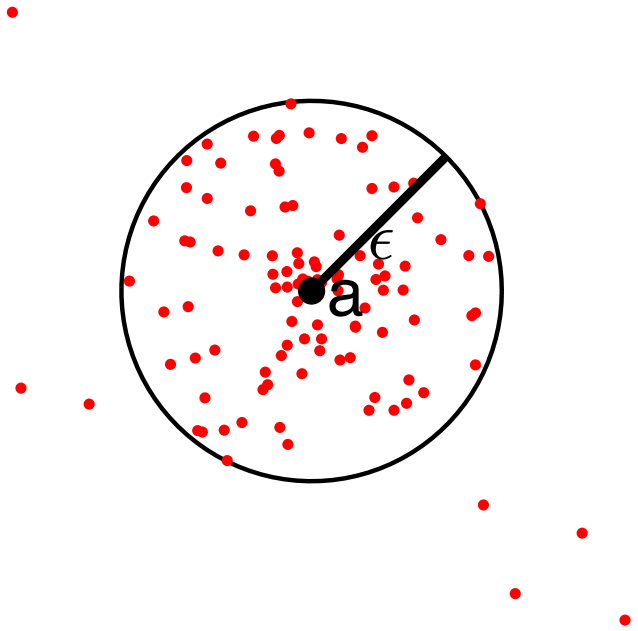
Analysis 1
— Grundlegende Vorbereitungen —

Armin Iske
www.math.uni-hamburg.de/home/iske



- Aussagen ($\rightsquigarrow$ lineare Algebra)
- Mengen
- Zahlenbereiche: von $\mathbb{N}$ bis $\mathbb{R}$
- komplexe Zahlen ($\rightsquigarrow$ lineare Algebra)
- Beweistechniken

1 Mengen

Definition: *Eine* Menge *ist eine Kollektion von paarweise verschiedenen Objekten. Die einzelnen Objekte werden* Elemente *der Menge genannt.* ◯

Beispiele für Mengen.

- $\mathbb{N} = \{1, 2, 3, \ldots\}$ Menge der natürlichen Zahlen;
- $\mathbb{N}_0 = \{0, 1, 2, 3, \ldots\}$ Menge der nicht-negativen ganzen Zahlen;
- Studierende der UHH;
- Studierende der Analysis I im WS 2022/2023 an der UHH;
- Menge der Primzahlen.

Notationen: Sei M eine Menge.

$$a \in M \iff a \text{ ist ein Element der Menge } M$$
$$a \notin M \iff \neg(a \in M)$$

Definition von Mengen.

- Aufzählung der Elemente: $M := \{1, 2, 3, 4\}$
- Charakterisierende Eigenschaft der Menge, $M := \{x \in \Omega \mid A(x)\}$

Bedeutung der verwendeten Symbole.

$:=$ "wird definiert durch"

$A(x)$ Aussageform, definiert für Elemente x aus einem `Grundbereich` Ω

Teilmengen von Mengen.

$$M \subset N \iff \forall x : (x \in M \Longrightarrow x \in N)$$

Gleichheit von Mengen.

$$M = N \iff \forall x : (x \in M \Longleftrightarrow x \in N)$$

Die leere Menge. Menge, die kein Element enthält. Bezeichnung: $\emptyset$

Ordnungseigenschaften.

- $M \subset M$;
- $(M \subset N) \wedge (N \subset M) \quad \Longrightarrow \quad M = N$;
- $(M \subset N) \wedge (N \subset P) \quad \Longrightarrow \quad M \subset P$.

Verknüpfung von Mengen.

$$\begin{aligned}
M \cup N &:= \{x \,|\, x \in M \vee x \in N\} && \text{(Vereinigung)} \\
M \cap N &:= \{x \,|\, x \in M \wedge x \in N\} && \text{(Durchschnitt)} \\
M \setminus N &:= \{x \,|\, x \in M \wedge x \notin N\} && \text{(Differenz)} \\
M \times N &:= \{(a,b) \,|\, a \in M \wedge b \in N\} && \text{(kartesisches Produkt)}
\end{aligned}$$

Definition: Für eine Menge M wird die Menge

$$\mathcal{P}(M) := \{X \,|\, X \subset M\}$$

aller Teilmengen von M als Potenzmenge von M bezeichnet. ◯

Bemerkungen und weitere Bezeichnungen.

- Gilt $M \cap N = \emptyset$, so nennt man M und N disjunkt.
- Verknüpfung von endlich vielen Mengen.

$$\begin{aligned}
\bigcup_{k=1}^{n} A_k &= A_1 \cup A_2 \cup \cdots \cup A_n \\
&:= \{a \mid \exists\, k \in \{1, \ldots, n\} : a \in A_k\} \\
\bigcap_{k=1}^{n} A_k &= A_1 \cap A_2 \cap \cdots \cap A_n \\
&:= \{a \mid \forall\, k \in \{1, \ldots, n\} : a \in A_k\} \\
\prod_{k=1}^{n} A_k &= A_1 \times A_2 \times \cdots \times A_n \\
&:= \{(a_1, \ldots, a_n) \mid \forall\, k \in \{1, \ldots, n\} : a_k \in A_k\}
\end{aligned}$$

Weitere Bemerkungen und Bezeichnungen.

- Für geordnete Paare bzw. n-Tupel gilt:

$$(a_1, a_2) = (b_1, b_2) \iff a_1 = b_1 \wedge a_2 = b_2$$
$$(x_1, \ldots, x_n) = (y_1, \ldots, y_n) \iff \forall k \in \{1, \ldots, n\} : x_k = y_k$$

- Beispiele für kartesische Produkte:
  - die euklidische Ebene

$$\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(x, y) \mid x, y \in \mathbb{R}\}$$

  - der dreidimensionale euklidische Raum

$$\mathbb{R}^3 = \mathbb{R} \times \mathbb{R} \times \mathbb{R} = \{(x, y, z) \mid x, y, z \in \mathbb{R}\}$$

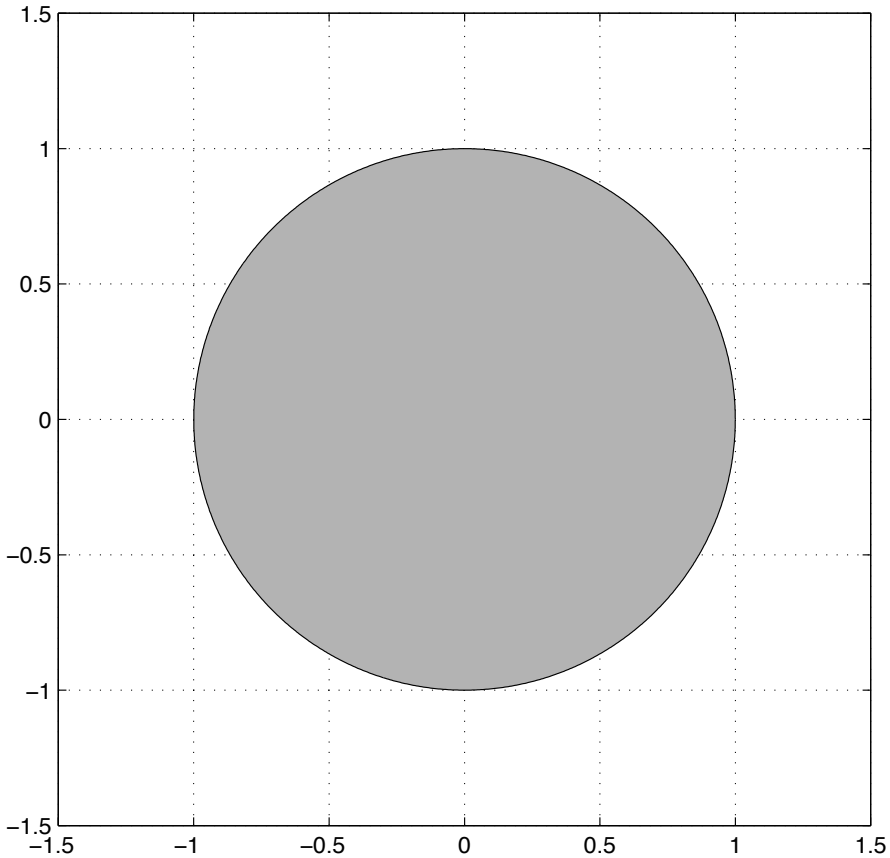
  - der n-dimensionale euklidische Raum

$$\mathbb{R}^n = \underbrace{\mathbb{R} \times \cdots \times \mathbb{R}}_{n\text{-fach}} = \{(x_1, \ldots, x_n) \mid x_k \in \mathbb{R} \text{ für alle } 1 \leq k \leq n\}$$

Der Einheitskreis.

- Kreisscheibe mit Radius 1 (Einheitskreis)

$$A := \left\{ (x, y) \in \mathbb{R}^2 \mid \sqrt{x^2 + y^2} \leq 1 \right\}$$



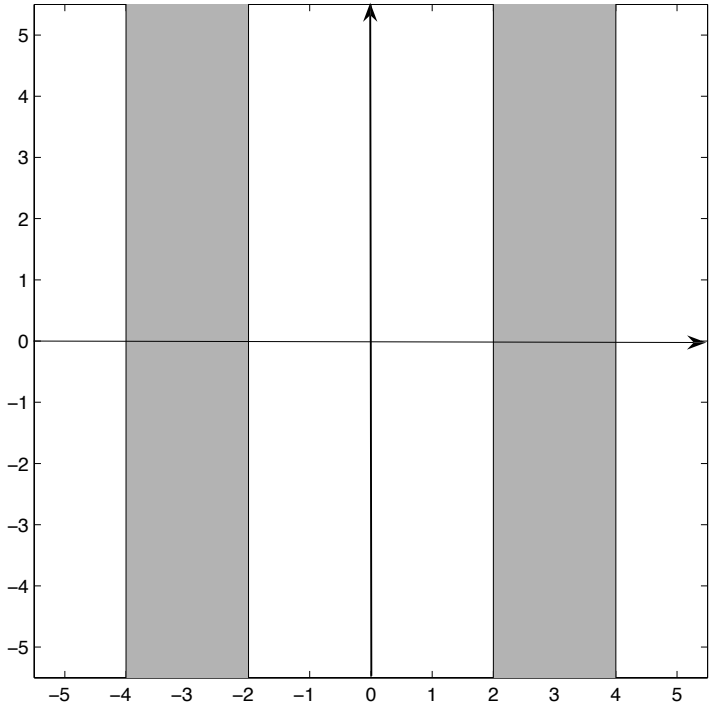
Zwei Streifen. $B := \{(x,y) \in \mathbb{R}^2 \mid 5 \leq x^2 + 1 \leq 17\}$

Beachte:

$$5 \leq x^2 + 1 \leq 17 \iff 4 \leq x^2 \leq 16 \iff -4 \leq x \leq -2 \vee 2 \leq x \leq 4$$

und somit gilt

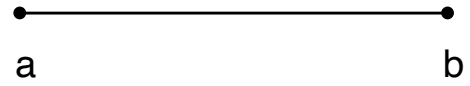
$$B = \{(x,y) \in \mathbb{R}^2 \mid -4 \leq x \leq -2 \vee 2 \leq x \leq 4\}.$$



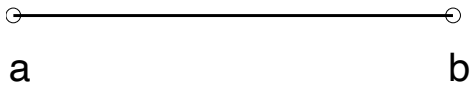
Intervalle in $\mathbb{R}$.

Seien $a, b \in \mathbb{R}$ mit $a < b$.

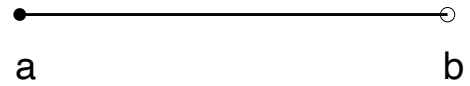
$$[a,b] := \{x \mid a \le x \le b\}$$ abgeschlossenes Intervall



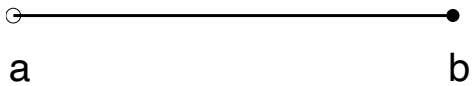
$$(a,b) := \{x \mid a < x < b\}$$ offenes Intervall



$$[a,b) := \{x \mid a \le x < b\}$$ halboffenes Intervall



$$(a,b] := \{x \mid a < x \le b\}$$ halboffenes Intervall



2 Zahlenbereiche – von natürlich bis reell

2.1 Natürliche Zahlen

Wir führen die aus der Schule bekannte Menge $\mathbb{N} = \{1, 2, 3, \ldots\}$ der natürlichen Zahlen hier formal durch die Axiome von Peano[a] (1889) ein.

Definition: Die natürlichen Zahlen sind eine Menge $\mathbb{N}$ mit einem ausgezeichneten Element $1 \in \mathbb{N}$, so dass folgende Eigenschaften gelten.

(P1) Jedes Element aus $\mathbb{N}$ besitzt einen eindeutigen Nachfolger in $\mathbb{N}$;

(P2) 1 ist kein Nachfolger zu einem Element in $\mathbb{N}$;

(P3) verschiedene Elemente aus $\mathbb{N}$ besitzen verschiedene Nachfolger;

(P4) Für $M \subset \mathbb{N}$ gilt das Vollständigkeitsaxiom: Falls $1 \in M$, und falls für jedes Element in M ebenso sein Nachfolger in M liegt, so gilt $M = \mathbb{N}$.

○

[a] Giuseppe Peano (1858-1932), italienischer Mathematiker

Reformulierung der Peano-Axiome

Wir wollen mit folgender Notation die Addition in $\mathbb{N}$ vorbereiten.

Definition: Für $n \in \mathbb{N}$ bezeichnen wir den Nachfolger von n mit $n+1$. ◯

Bemerkung: Mit dieser Definition können wir die Peano-Axiome reformulieren:
Die Menge $\mathbb{N}$ der natürlichen Zahlen erfüllt folgende Eigenschaften.

- $1 \in \mathbb{N}$;
- $n \in \mathbb{N} \Longrightarrow n+1 \in \mathbb{N}$ für alle $n \in \mathbb{N}$;
- $n \neq m \Longrightarrow n+1 \neq m+1$ für alle $n, m \in \mathbb{N}$;
- $n \in \mathbb{N} \Longrightarrow n+1 \neq 1$ für alle $n \in \mathbb{N}$;
- Für $M \subset \mathbb{N}$ gilt das Vollständigkeitsaxiom:

$$1 \in M \wedge (\forall n \in M : [n \in M \Longrightarrow (n+1) \in M]) \quad \Longrightarrow \quad M = \mathbb{N}.$$

□

Addition in $\mathbb{N}$. Wir führen die Addition '$+$' in $\mathbb{N}$ wie folgt ein:

- Für $n \in \mathbb{N}$ liefert die Addition von 1 und n den Nachfolger $n+1$ von n.
- Für $n, m \in \mathbb{N}$ ist die Addition von n und m erklärt durch die m-fache Anwendung der Addition der 1 auf n. Wir bezeichnen diese Addition als Summe der Summanden n und m, kurz: $n+m$, wobei

$$n + m = (\cdots((n + \underbrace{1) + 1) + 1 \ldots) + 1}_{m}.$$

Multiplikation in $\mathbb{N}$. Wir führen die Multiplikation '$\cdot$' in $\mathbb{N}$ so ein:

- Für $n, m \in \mathbb{N}$ ist die Multiplikation von n mit m erklärt durch die m-fache Addition von n. Wir bezeichnen diese Multiplikation als Produkt der Faktoren n und m, kurz: $n \cdot m$, wobei

$$n \cdot m = \underbrace{n + \ldots + n}_{m}.$$

Rechenregeln der Addition und Multiplikation in $\mathbb{N}$.

Rechenregeln der Addition: Für $n, m, k \in \mathbb{N}$ gilt:

- $n + m = m + n$ Kommutativgesetz;
- $k + (n + m) = (k + n) + m$ Assoziativgesetz.

Rechenregeln der Multiplikation: Für $n, m, k \in \mathbb{N}$ gilt:

- $n \cdot m = m \cdot n$ Kommutativgesetz;
- $k \cdot (n \cdot m) = (k \cdot n) \cdot m$ Assoziativgesetz.

Schließlich gilt für $n, m, k \in \mathbb{N}$ das Distributivgesetz:

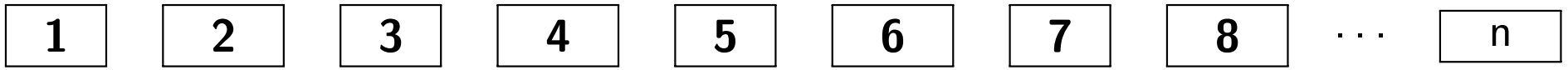
$$k \cdot (n + m) = k \cdot n + k \cdot m.$$

Zur Mächtigkeit der natürlichen Zahlen.

Paradoxes Gedankenexperiment: Das Hilbert[a]-Hotel.

Voraussetzungen:

- Das Hilbert-Hotel hat unendlich viele Zimmer.
- Die Zimmer sind durchnummiert mit den natürlichen Zahlen bei 1 beginnend.



Szenario: Kommt ein neuer Gast ins Hilbert-Hotel . . .

. . . aber alle Zimmer im Hilbert-Hotel sind leider belegt.

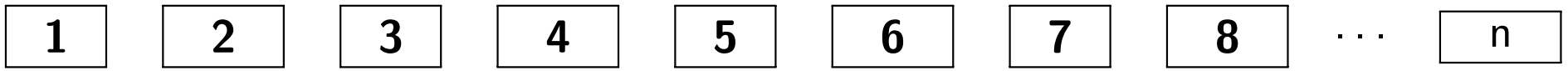
Frage: Kann der neue Gast noch untergebracht werden?

[a] David Hilbert (1862-1943), deutscher Mathematiker

Szenario 1: $1 + \infty = \infty$.

Ausgangspunkt: Kommt ein neuer Gast ins Hilbert-Hotel . . .

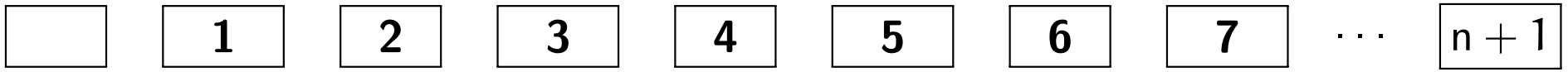
. . . aber alle Zimmer im Hilbert-Hotel sind leider belegt.



Frage: Kann der neue Gast noch untergebracht werden?

Antwort: klar doch!

Mit dem Umzug $k \mapsto k+1$ der aktuellen Gäste . . . in das Nachfolger-Zimmer . . .
. . . und dem Einzug des neuen Gastes in Zimmer 1.



Szenario 2: $\infty + \infty = \infty$.

Ausgangspunkt: Kommt ein voller Bus mit *unendlich abzählbar vielen* Gästen beim Hilbert-Hotel an . . . aber alle Zimmer im Hilbert-Hotel sind leider belegt.

1	2	3	4	5	6	7	8	· · ·	n

Frage: Können die Gäste noch untergebracht werden?

Antwort: klar doch!

Mit dem Umzug $k \mapsto 2k$ der aktuellen Gäste . . . in die geraden Zimmer
. . . und dem Einzug $\ell \mapsto 2\ell - 1$ der neuen Gäste . . . in die ungeraden Zimmer.

	2		4		6		8	· · ·	2n

Bemerkung: Damit bleibt kein Zimmer leer.

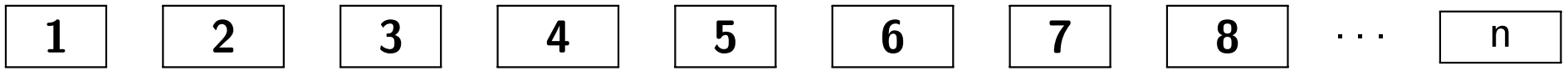
Szenario 3: $\infty \cdot \infty + \infty = \infty$.

Ausgangspunkt: Kommen unendlich viele Busse mit unendlich vielen Gästen an

Genauer:

. . . abzählbar unendlich viele Busse mit jeweils abzählbar unendlich vielen Gästen.

. . . aber alle Zimmer im Hilbert-Hotel sind leider belegt.



Frage: Können die Gäste noch untergebracht werden?

. . . so dass danach alle Zimmer belegt sind.

Antwort: klar doch! $\rightsquigarrow$ Aufgabe des Tages.

2.2 Primzahlen

Definition: Eine natürliche Zahl $m \in \mathbb{N}$ heißt Teiler von $n \in \mathbb{N}$, falls ein $k \in \mathbb{N}$ existiert mit

$$n = k \cdot m,$$

und wir notieren dies kurz mit $m|n$. ◯

Beobachtung: Jedes $n \in \mathbb{N}$ besitzt offensichtlich die beiden (*trivialen*) Teiler 1 und n, denn es gilt

$$n = n \cdot 1 = 1 \cdot n.$$

Definition: Eine natürliche Zahl $p \geq 2$, die nur die trivialen Teiler 1 und p besitzt, heißt Primzahl, kurz gesagt: p ist prim.
Wir bezeichnen die Menge der Primzahlen mit $\mathbb{P}$. ◯

Bemerkung: Per Definition ist jede Primzahl eine natürliche Zahl, und daher gilt die Inklusion $\mathbb{P} \subset \mathbb{N}$. Die ersten Primzahlen lauten $2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots$

Der Fundamentalsatz der Arithmetik.

Theorem (Fundamentalsatz der Arithmetik)**:** *Jede natürliche Zahl* $n \in \mathbb{N}$ *lässt sich als Produkt*

$$n = p_1^{r_1} \cdot p_2^{r_2} \cdot \ldots \cdot p_k^{r_k},$$

von Primzahlpotenzen *schreiben, mit paarweise verschiedenen Primzahlen* $p_j \in \mathbb{P}$ *und mit Exponenten* $r_j \in \mathbb{N}$*, für* $1 \leq j \leq k$*. Diese Darstellung heißt* Primfaktorzerlegung *von* n*.* □

Wir führen den (einfachen) Beweis dieser wichtigen Aussage hier nicht, da wir erst später über Beweise und Beweistechniken reden wollen.

Wir schließen die Vorbereitungen mit zwei Bemerkungen (ebenso ohne Beweise).

Bemerkung 1: Die Primzahlbasen $p_1, \ldots, p_k$ und die zugehörigen Exponenten $r_1, \ldots, r_k \geq 1$ der Primfaktorzerlegung von n sind eindeutig. □

Bemerkung 2: Es gibt unendlich viele Primzahlen. □

2.3 Ganze Zahlen

Motivation: Wollen für $a, b \in \mathbb{N}$ (lineare) Gleichungen der Form

$$a + n = b$$

in $\mathbb{N}$ lösen, d.h. wir suchen $n \in \mathbb{N}$ mit $a + n = b$.

Problem i.A. nicht in $\mathbb{N}$ lösbar, sondern nur falls $a < b$.

Erweiterung der natürlichen Zahlen:

- Wir führen `die Null` als *neutrales Element der Addition* ein, so dass

  $$a + 0 = 0 + a = a$$

  für alle $a \in \mathbb{N}$ gilt.
- Wir führen zu jedem $n \in \mathbb{N}$ eine `additive Gegenzahl` $-n$ ein, für die gilt

  $$n + (-n) = (-n) + n = 0.$$
- Im Folgenden setzen wir $n - m := n + (-m)$, für $n, m \in \mathbb{N}$ (bzw. $\mathbb{Z}$).

Die ganzen Zahlen und ihre algebraische Struktur.

Wir führen die Menge der ganzen Zahlen $\mathbb{Z}$ ein als die Vereinigung

$$\mathbb{Z} := -\mathbb{N} \cup \{0\} \cup \mathbb{N}$$

wobei $-\mathbb{N}$ die Menge aller additiven Gegenzahlen zu den Elementen aus $\mathbb{N}$ ist.

Die Menge $\mathbb{Z}$ bildet mit der Addition eine Abelsche[a] Gruppe, d.h. in $\mathbb{Z}$ gilt:

- $n + m = m + n$ Kommutativgesetz;
- $k + (n + m) = (k + n) + m$ Assoziativgesetz;
- $n + 0 = 0 + n = n$ Existenz eines neutralen Elements;
- $n + (-n) = (-n) + n = 0$ Existenz eines inversen Elements.

Damit ist die Gleichung $a + n = b$ stets in $\mathbb{Z}$ lösbar mit $n = b + (-a) := b - a$.

Bemerkung: Für die Multiplikation in $\mathbb{Z}$ gelten Regeln wie in $\mathbb{N}$, und genauso gilt das Distributivgesetz in $\mathbb{Z}$; $(\mathbb{Z}, +, \cdot)$ wird damit als Ring bezeichnet. □

[a] Niels Henrik Abel (1802-1829), norwegischer Mathematiker

2.4 Rationale Zahlen

Die *rationalen Zahlen* werden in der Schule häufig als *Bruchzahlen* bezeichnet.

Wir definieren die Menge der `rationalen Zahlen` formal mit

$$\mathbb{Q} := \left\{ \frac{m}{n} \,\middle|\, m \in \mathbb{Z}, n \in \mathbb{N} \right\}.$$

Für die rationalen Zahlen führen wir Addition und Multiplikation wie folgt ein:

- Die `Addition` '$+$'

$$\frac{n}{m} + \frac{k}{\ell} := \frac{n \cdot \ell + k \cdot m}{m \cdot \ell} \qquad \text{für } n, k \in \mathbb{Z} \text{ und } m, \ell \in \mathbb{N}.$$

- Die `Multiplikation` '$\cdot$'

$$\frac{n}{m} \cdot \frac{k}{\ell} := \frac{n \cdot k}{m \cdot \ell} \qquad \text{für } n, k \in \mathbb{Z} \text{ und } m, \ell \in \mathbb{N}.$$

Dabei haben wir die entsprechenden Verknüpfungen '$+$' und '$\cdot$' in $\mathbb{N}$ bzw. in $\mathbb{Z}$ verwendet. Die Verknüpfungen sollten mit Rechenregeln bereits bekannt sein.

2.5 Reelle Zahlen

Wir beginnen mit einem wichtigen Resultat, das wir erst später beweisen werden.

Proposition: Die Gleichung $x^2 = 2$ besitzt keine Lösung in $\mathbb{Q}$. □

Ausblick: Wir wollen im Folgenden die rationalen Zahlen $\mathbb{Q}$ erweitern durch die *reellen Zahlen* $\mathbb{R}$, so dass die Gleichung $x^2 = 2$ in $\mathbb{R}$ lösbar ist. Die (eindeutige) positive Lösung dieser Gleichung bezeichnen wir mit $\sqrt{2}$. Damit lässt sich das obige Resultat kurz reformulieren als: $\sqrt{2} \notin \mathbb{Q}$.

Wir schließen unsere ausblickende Diskussion wie folgt.

Bemerkung: Die Zahl $\sqrt{2}$ lässt sich beliebig genau durch rationale Zahlen aus $\mathbb{Q}$ *approximieren* (*annähern*), d.h. zu jedem $\epsilon > 0$ gibt es ein $q \in \mathbb{Q}$ mit

$$|\sqrt{2} - q| < \epsilon.$$

Bemerkung: Wir notieren (etwas lax), dass die Menge $\mathbb{R}$ der reellen Zahlen aus allen Zahlen besteht, die sich beliebig gut durch rationale Zahlen approximieren lassen. Insbesondere gilt $\mathbb{Q} \subset \mathbb{R}$. Wir werden diese Aussage später präzisieren. □

Axiomensystem für die reellen Zahlen.

(I) Regeln der Addition (Abelsche Gruppe):

$$
\begin{array}{lllll}
\text{(a)} & x+(y+z) & = & (x+y)+z & \\
\text{(b)} & x+y & = & y+x & \\
\text{(c)} & x+0 & = & 0+x & = \quad x \\
\text{(d)} & x+(-x) & = & (-x)+x & = \quad 0
\end{array}
$$

(II) Regeln der Multiplikation:

$$
\begin{array}{lllll}
\text{(a)} & x\cdot(y\cdot z) & = & (x\cdot y)\cdot z & \\
\text{(b)} & x\cdot y & = & y\cdot x & \\
\text{(c)} & x\cdot 1 & = & 1\cdot x & = \quad x, \text{ wobei } 1\neq 0 \\
\text{(d)} & x\cdot\left(\frac{1}{x}\right) & = & \left(\frac{1}{x}\right)\cdot x & = \quad 1 \quad \text{für } x\neq 0
\end{array}
$$

(III) Distributivgesetz: $x\cdot(y+z)=x\cdot y+x\cdot z$

(IV) Anordnungsaxiome: In $\mathbb{R}$ sind bestimmte Elemente als positiv, andere als negativ ausgezeichnet, so dass die Anordnungsaxiome gelten:

(A1) Für jede reelle Zahl $x \in \mathbb{R}$ gilt genau eine der drei Eigenschaften:
$x > 0$ (positiv) oder $x = 0$ (Null) oder $x < 0$ (negativ).

(A2) Für $x, y \in \mathbb{R}$ gilt: Sind $x > 0$ und $y > 0$, so folgt $x + y > 0$.

(A3) Für $x, y \in \mathbb{R}$ gilt: Sind $x > 0$ und $y > 0$, so folgt $x \cdot y > 0$.

Definition: Für $x, y \in \mathbb{R}$ notieren wir $x > y$, falls $x - y > 0$. Weiterhin notieren wir $x \geq y$, falls $x > y$ oder $x = y$. Statt $x > y$ (oder $x \geq y$) notieren wir genauso $y < x$ (bzw. $y \leq x$). ◯

(V) Vollständigkeitsaxiom (Dedekind[a], 1872)**:**

Sei $\mathbb{R} = L \cup R$ zerlegt in nichtleere Mengen $L, R \neq \emptyset$ mit $\forall\, x \in L,\, y \in R : x < y$.

Dann gibt es genau eine Schnittzahl $s \in \mathbb{R}$ mit

$$\forall\, x \in L,\, y \in R : \quad x \leq s \leq y.$$

[a] Richard Dedekind (1831-1916), deutscher Mathematiker

Bemerkungen und Bezeichnungen.

- Eine nichtleere Menge mit (I) heißt `Abelsche Gruppe`.
- Eine nichtleere Menge mit (I)–(III) heißt `Körper`.
- Ein Körper mit (IV) heißt `angeordneter Körper`.
- Die rationalen Zahlen $\mathbb{Q}$ bilden einen angeordneten Körper.
- **ABER:** Die rationalen Zahlen erfüllen nicht das Vollständigkeitsaxiom!

DENN: Für

$$\begin{aligned} L &:= \{x \in \mathbb{Q} \mid x^2 < 2 \vee x < 0\} \\ R &:= \{x \in \mathbb{Q} \mid x^2 > 2 \wedge x > 0\} \end{aligned}$$

gibt es keine Schnittzahl in $\mathbb{Q}$, denn die Schnittzahl $s = \sqrt{2} \in \mathbb{R}$ liegt nicht in $\mathbb{Q}$.

□

Direkte Folgerungen aus den Anordnungsaxiomen.

Aus den Anordnungsaxiomen **(A1)-(A3)** folgen weitere *Ordnungseigenschaften*:

(a) $x < 0$ ist gleichbedeutend mit $-x > 0$, denn:
Mit $x < 0$ gilt (per Definition) $0 > x$, und damit (erneut per Definition) $0 - x > 0$, d.h. $-x > 0$. Genauso: aus $-x > 0$ folgt $x < 0$ (Übung).

(a)′ $x \leq y$ ist gleichbedeutend mit $-x \geq -y$, denn: Entweder ist $x = y$, und dann ist die Aussage trivial. Oder es gilt $x < y$ bzw. $x - y < 0$, und dann folgt die Aussage aus (a) mit $-x + y > 0$ bzw. $-x > -y$.

(b) Aus $x < y$ und $y < z$ folgt $x < z$ (`Transitivität`), denn:
Nach Voraussetzung gelten $y - x > 0$ und $z - y > 0$.
Aus **(A2)** folgt damit $(y - x) + (z - y) = z - x > 0$ bzw. $x < z$.

(c) Aus $x < y$ und $a \in \mathbb{R}$ folgt $a + x < a + y$, denn nach Voraussetzung:
$(a + y) - (a + x) = y - x > 0$, und somit $a + x < a + y$.

(c)′ Aus $x < y$ und $x' < y'$ folgt $x + x' < y + y'$, denn aus (c) folgt
$x + x' < y + x'$ und $y + x' < y + y'$, somit $x + x' < y + y'$ wegen (b).

Zusammenfassung von Ordnungseigenschaften in $\mathbb{R}$

(a) $x < 0$ ist gleichbedeutend mit $-x > 0$.

(b) Aus $x < y$ und $y < z$ folgt $x < z$ (Transitivität).

(c) Gilt $x < y$ so folgt $a + x < a + y$ für jedes $a \in \mathbb{R}$.

(d) Aus $x < y$ und $x' < y'$ folgt $x + x' < y + y'$.

(e) Gilt $x < y$ und $a > 0$, so folgt $a \cdot x < a \cdot y$.

(f) Aus $0 \leq x < y$ und $0 \leq a < b$ folgt $a \cdot x < b \cdot y$.

(g) Gilt $x < y$ und $a < 0$, so folgt $a \cdot x > a \cdot y$.

(h) Für jedes $x \neq 0$ gilt $x^2 > 0$.

(i) Ist $x > 0$ (bzw. $x < 0$), so ist auch $1/x > 0$ (bzw. $1/x < 0$).

(j) Aus $0 < x < y$ folgt $1/x > 1/y$.

(k) Es gilt $1 > 0$.

3 Beweistechniken

Ziel: Wir wollen mathematische Aussagen verifizieren oder falsifizieren.

Methode: Der mathematische Beweis.

Grundelemente mathematischer Texte:

- **Axiome:** Grundannahmen, die nicht bewiesen werden.
- **Definition:** Festlegung von Begriffen und Notationen.
  Definitionen sind keine Aussagen, werden daher nicht bewiesen.
- **Mathematische Aussagen müssen bewiesen werden!**
  Theorem/Satz, **Lemma/Hilfssatz**, **Korollar/Folgerung**, **Proposition**.
- **Bemerkung:** Erläuterung oder (zusätzliche) Erklärung zur Motivation
- **Beispiel:** Zur weiteren Illustration von Aussagen oder Begriffen

Im Folgenden diskutieren wir verschiedene Beweistechniken, die wir auf mathematische Aussagen (bzw. Behauptungen) exemplarisch anwenden.

3.1 Gegenbeispiel

Typische Situation: Wir wollen eine mathematische Aussage falsifizieren.

Beweismethode:
Mit einem `Gegenbeispiel` wird eine mathematische `Hypothese` widerlegt.

Ein einfaches Beispiel.

Behauptung: Alle Primzahlen sind ungerade: $\forall p \in \mathbb{P} : p$ ungerade.

Diese Aussage ist offenbar falsch.

Beweis durch Gegenbeispiel: Grundlegende Analyse: Es gilt die Äquivalenz

$$\neg\,(\forall\, p \in \mathbb{P} : p \text{ ungerade}) \quad \Longleftrightarrow \quad \exists\, p \in \mathbb{P} : \neg\,(p \text{ ungerade})\,.$$

und dies führt uns sofort zum Beleg: Die Zahl 2 ist prim, aber nicht ungerade.

Daher sind nicht alle Primzahlen ungerade. Die 2 ist ein `Gegenbeispiel`. □

Die Collatz $(3n+1)$-Vermutung.

Die Collatz[a]-Vermutung bezieht sich auf Folgen in $\mathbb{N}$, die so erzeugt werden:

Für $n \in \mathbb{N}$ wird die jeweils nächste Zahl $n^+ \in \mathbb{N}$ dieser Folge bestimmt durch

$$n^+ := \begin{cases} n/2 & \text{falls } n \text{ gerade;} \\ 3n+1 & \text{falls } n \text{ ungerade.} \end{cases}$$

Startet man beispielsweise mit $n = 19$, so erhält man die Folge

$$19, 58, 29, 88, 44, 22, 11, 34, 17, 52, 26, 13, 40, 20, 10, 5, 16, 8, 4, 2, 1, 4, 2, 1, 4, 2, 1, \ldots$$

Vermutung (Collatz, 1937): *Jede so konstruierte Zahlenfolge mündet in den Zyklus 4, 2, 1, egal, mit welcher natürlichen Zahl $n > 0$ man beginnt.* □

Trotz zahlreicher Anstrengungen und hochdotierter ausgelobter Preise ist die Vermutung immer noch offen, d.h. das Collatz $(3n+1)$-Problem ist ungelöst. Ein Gegenbeispiel würde reichen, um die Vermutung von Collatz zu falsifizieren. Alle natürlichen Zahlen bis zur Größenordnung 10^{24} wurden bereits überprüft. □

[a] Lothar Collatz (1910-1990), Hamburger Mathematiker

3.2 Direkter Beweis

Ein direkter Beweis ist wie folgt strukturiert.

Unter der *Voraussetzung* (Prämisse) einer Aussage A folgt als *Behauptung* (Konklusion) eine andere Aussage B, d.h. wir zeigen die Implikation

$$A \quad \Longrightarrow \quad B \qquad \text{für Aussagen } A, B$$

unter Anwendung der Aussagenlogik.

In einem Kettenschluss besteht ein direkter Beweis aus mehreren Implikationen:

$$A = A_0 \Longrightarrow A_1 \Longrightarrow A_2 \Longrightarrow \ldots \Longrightarrow A_n = B,$$

für Aussagen $A_0, A_1, \ldots, A_n$, und daraus resultiert insbesondere die Implikation

$$A \quad \Longrightarrow \quad B.$$

□

Ein einfaches Beispiel für einen direkten Beweis.

Behauptung: Sei $n \in \mathbb{N}$ gerade. Dann ist n^2 gerade.

Direkter Beweis: Sei $n \in \mathbb{N}$ gerade. Dann ist die Zahl 2 Teiler von n, $2|n$, d.h. es gibt ein $k \in \mathbb{N}$ mit $n = 2 \cdot k$. Daraus folgt

$$n^2 = (2 \cdot k)^2 = 4 \cdot k^2 = 2 \cdot (2 \cdot k^2).$$

Somit wird n^2 von 2 geteilt, $2|n^2$, d.h. n^2 ist gerade. ■

Ein weiteres Beispiel für einen direkten Beweis.

Behauptung: Für positive reelle Zahlen $a, b > 0$ gilt die Ungleichung zwischen dem geometrischen und dem arithmetischen Mittel, d.h. es gilt

$$\sqrt{a \cdot b} \leq \frac{a+b}{2} \qquad \text{für alle } a, b > 0.$$

Direkter Beweis: Seien $a, b > 0$ positive reelle Zahlen. Dann sind die Quadratwurzeln $\sqrt{a}, \sqrt{b}$ wohldefiniert. Nun gilt die Ungleichung

$$0 \leq \left(\sqrt{a} - \sqrt{b}\right)^2 = a - 2 \cdot \sqrt{a} \cdot \sqrt{b} + b$$

und daraus folgt sofort

$$\sqrt{a \cdot b} \leq \frac{a+b}{2},$$

womit die Behauptung bewiesen ist. ■

Direkte Beweise für Ordnungseigenschaften.

Wir hatten Ordnungseigenschaften diskutiert, die aus den Ordnungsaxiomen (A1)-(A3) folgen. Wir führen hierzu direkte Beweise exemplarisch wie folgt.

Behauptung: Für reelle Zahlen $x, y \in \mathbb{R}$ gelten die folgenden Aussagen.

(a) $x^2 > 0$ für $x \neq 0$.

Beweis: Falls $x > 0$, so folgt $x \cdot x > 0$ aus **(A3)**.
Falls $x < 0$, so folgt $x^2 = (-x) \cdot (-x) > 0$ erneut aus **(A3)**.

(b) Ist $x > 0$ (bzw. $x < 0$), so ist auch $1/x > 0$ (bzw. $1/x < 0$).

Beweis: Es gilt $1/x = x \cdot (1/x)^2$, und weiterhin $(1/x)^2 > 0$ wegen (a).
Falls $x > 0$, so folgt $1/x = x \cdot (1/x)^2 > 0$, also $1/x > 0$.
Falls $x < 0$, so folgt $1/x = x \cdot (1/x)^2 < 0$, also $1/x < 0$.

(c) Aus $0 < x < y$ folgt $0 < 1/y < 1/x$.

Beweis: Mit $x > 0$ und $y > 0$ gilt $xy > 0$ wegen **(A3)**. Aus (b) folgt daraus $1/(xy) = 1/x \cdot 1/y > 0$. Nach Multiplikation beider Seiten in $x < y$ mit $1/(xy) > 0$ folgt schließlich $1/y = x(1/x \cdot 1/y) < y(1/x \cdot 1/y) = 1/x$. ■

3.3 Indirekter Beweis

Grundlage: Die Tautologie der Kontraposition (d.h. des Widerspruchs)

$$A \Longrightarrow B \qquad \Longleftrightarrow \qquad \neg B \Longrightarrow \neg A.$$

Daraus resultiert die Beweismethode des indirekten Beweises:

Zum Beweis der Implikation

$$A \quad \Longrightarrow \quad B$$

beweisen wir die Implikation

$$\neg B \quad \Longrightarrow \quad \neg A.$$

- Dazu nehmen wir die Gültigkeit der Aussage $\neg B$ an.
- Dann folgern wir (unter der Prämisse $\neg B$) die Gültigkeit von $\neg A$.
- Dies steht jedoch im Widerspruch zur Prämisse A (in $A \Longrightarrow B$).

Bemerkung: Diese Beweistechnik heißt ebenso Widerspruchsbeweis. □

Ein einfaches Beispiel für einen indirekten Beweis.

Behauptung: Für $n \in \mathbb{N}$ sei n^2 gerade. Dann ist n gerade.

Vorbemerkung:
Wir betrachten für $n \in \mathbb{N}$ die Aussagen A: „n^2 *gerade*“und B: „n *gerade*“.

Indirekter Beweis: Sei n^2 gerade (d.h. A sei wahr).

Wir zeigen die Implikation $\neg B \Longrightarrow \neg A$ wie folgt. Angenommen, n sei ungerade (d.h. $\neg B$ sei wahr). Dann $\exists k \in \mathbb{N} : n = 2k - 1$ und daraus folgt

$$n = 2k - 1 \quad \Longrightarrow \quad n^2 = (2k-1)^2 = 4k^2 - 4k + 1 = 2(2k^2 - 2k) + 1,$$

womit n^2 ungerade ist (d.h. $\neg A$ ist wahr). Dies steht allerdings im Widerspruch zur Prämisse der Aussage A (n^2 gerade). Damit ist die Behauptung bewiesen. ■

Folgerung: *Eine natürliche Zahl $n \in \mathbb{N}$ ist genau dann gerade, wenn ihr Quadrat n^2 gerade ist, d.h. für $n \in \mathbb{N}$ gilt die Äquivalenz*

$$n \text{ gerade} \qquad \Longleftrightarrow \qquad n^2 \text{ gerade.}$$

■

Ein weiteres Beispiel für einen indirekten Beweis.

Behauptung: *Die Zahl* $\sqrt{2}$ *ist irrational, d.h.* $\sqrt{2}$ *läßt sich nicht als Bruch* $\sqrt{2} = n/m$ *mit natürlichen Zahlen* $n, m \in \mathbb{N}$ *darstellen.*

Beweis durch Widerspruch: Annahme: $\exists n, m \in \mathbb{N} : \sqrt{2} = n/m$.

Wir nehmen ohne Einschränkung der Allgemeinheit (kurz: ohne Einschränkung) an, n und m seien teilerfremd. Anderenfalls teilen wir m, n durch deren größten gemeinsamen Teiler (ggT).

Unter der obigen Annahme $\sqrt{2} = n/m$ gilt:

$$2m^2 = n^2 \quad \Longrightarrow \quad n^2 \text{ gerade} \quad \Longrightarrow \quad n \text{ gerade} \quad \Longrightarrow \quad \exists k \in \mathbb{N} : n = 2k.$$

Einsetzen in $2m^2 = n^2$ ergibt:

$$2m^2 = n^2 = (2k)^2 = 4k^2 \Longrightarrow m^2 = 2k^2 \Longrightarrow m^2 \text{ gerade} \Longrightarrow m \text{ gerade.}$$

Dies ist ein Widerspruch zur Annahme, wonach n und m teilerfremd seien.

Die Annahme $\sqrt{2} = n/m$ ist somit falsch. Damit ist $\sqrt{2}$ eine irrationale Zahl. ■

Theorem (Satz von Euklid[a]): Es gibt unendlich viele Primzahlen.

Beweis durch Widerspruch: Angenommen, es gäbe nur *endlich* viele Primzahlen, $p_1, \ldots, p_n$, für $n \in \mathbb{N}$. Dann betrachten wir die Zahl

$$p = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1.$$

Zwischenbehauptung: Die Zahl p ist *nicht* durch p_j teilbar, für $j = 1, 2, \ldots, n$. Auch diese Aussage beweisen wir durch einen Widerspruchsbeweis: Angenommen, p wäre durch p_j teilbar. Dann gibt es eine Zahl $q \in \mathbb{N}$ mit

$$q \cdot p_j = p = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1.$$

Daraus folgt (nachdem wir p_j aus dem Produkt $p_1 \cdot \ldots \cdot p_n$ ausklammern und umformen)

$$1 = p_j \cdot (q - p_1 \cdot \ldots \cdot p_{j-1} \cdot p_{j+1} \cdot \ldots \cdot p_n)$$

und dies steht im Widerspruch zu $p_j \geq 2$.

Nach dieser Zwischenbehauptung taucht keine der Primzahlen $p_1, \ldots, p_n$ in der Primfaktorzerlegung von p auf. Nach unserer Annahme gibt es allerdings nur die Primzahlen $p_1, \ldots, p_n$. In diesem Fall besitzt p somit keine Primfaktorzerlegung. Dies steht jedoch im Widerspruch zum Fundamentalsatz der Arithmetik. Damit ist die Aussage bewiesen. ■

[a] Euklid von Alexandria (3. Jahrhundert v.Chr.), griechischer Mathematiker

3.4 Das Schubfachprinzip

Das Schubfachprinzip von Dirichlet[a] erklären wir wie folgt: Falls man $n \in \mathbb{N}$ Objekte auf $m \in \mathbb{N}$ Mengen verteilt, dann gibt es mindestens eine Menge,

(a) in der mehr als ein Objekt enthalten ist, falls $n > m$;

(b) in der keines dieser Objekte enthalten ist, falls $n < m$.

Wir beweisen diese Aussage jeweils per Widerspruch.

Beweis:

(b): Sei $n < m$. Angenommen, in jeder der m Mengen sei mindestens eines der n Objekte enthalten, so wurden mindestens m Objekte auf die Mengen verteilt. Daraus folgt $n \geq m$, und dies steht im Widerspruch zur Annahme $n < m$.

(a): Sei $n > m$. Angenommen, in keiner der m Mengen sei mehr als ein Objekt enthalten. Dann wurden auf die m Mengen insgesamt höchstens m Objekte verteilt, womit $n \leq m$. Dies steht im Widerspruch zur Annahme $n > m$. ■

[a] Johann Peter Gustav Lejeune Dirichlet (1805-1859), deutscher Mathematiker

Ein Beispiel zum Schubfachprinzip.

Nach einer statistischen Erhebung leben in Hamburg 1,899 Millionen Menschen, davon sind 7,9 % zwischen 18 und 24 Jahre alt. Weiterhin hat jeder Mensch aus dieser Altersgruppe zwischen 100.000 und 150.000 Haare auf dem Kopf.

Behauptung: Mindestens vier Hamburger Menschen im Alter zwischen 18 und 24 Jahren haben exakt gleich viele Haare auf dem Kopf.

Beweis: Nach Aufgabenstellung leben $1,899\text{Mio} \times 0,079 = 150.021$ Menschen im Alter von 18 bis 24 Jahren in Hamburg, wobei jeder zwischen 100.000 und 150.000 Haare auf dem Kopf hat. Somit gibt es $m = 50.001$ (= 150.000-100.000+1) *Schubfächer* (d.h. Mengen für die verschiedenen Zahlen der Kopfhaare), auf die die $n = 150.021$ Hamburger Menschen im Alter zwischen 18 und 24 Jahren verteilt werden können.

Mit $n = 150.021$ und $m = 50.001$ ist die Anzahl der Objekte (Hamburger Menschen im Alter zwischen 18 und 24 Jahren) sogar mehr als dreimal größer als die Anzahl der Schubfächer, auf die die Objekte verteilt werden. Aus dem Schubfachprinzip folgt, dass es mindestens ein Schubfach gibt, in dem mindestens vier Objekte liegen. ■

Noch ein Beispiel zum Schubfachprinzip.

Behauptung: Für jede natürliche Zahl $n \in \mathbb{N}$ gibt es ein (ganzzahliges) Vielfaches von n, dessen Ziffern nur aus Nullen und Einsen bestehen.

Beweis: Wir wenden das Schubfachprinzip wie folgt an.

Vorüberlegung: Bei der Division einer beliebigen natürlichen Zahl durch n sind bei dieser Teilung n verschiedene Reste möglich, nämlich von 0 bis $n-1$.

Wir sehen uns nun $n+1$ Zahlen an, die sämtlich nur aus der Ziffer 1 bestehen. Die kleinste lautet 1, die nächste 11 und so weiter bis zur größten, die aus $n+1$ Einsen besteht. Für diese $n+1$ Zahlen sind beim Teilen durch n höchstens n verschiedene Reste möglich. Es muss also mindestens zwei Zahlen geben, die den gleichen Rest besitzen. Subtrahieren wir diese beiden voneinander, entsteht eine Zahl der Form $11111\ldots00000$. Sie hat vorn nur Einsen und hinten nur Nullen — und sie ist durch n teilbar. ■

3.5 Fallunterscheidung

Beweismethode: Zerlege die Annahme über die relevanten Objekte in mehrere separate Einzelfälle, für die die Behauptung dann jeweils bewiesen werden. Diese Zerlegung muss allerdings alle möglichen Einzelfälle für die Objekte abdecken.

Wir betrachten nun ein Beispiel, wobei wir den Betrag $|x|$ von $x \in \mathbb{R}$ verwenden:

$$|x| := \begin{cases} x & \text{für } x \geq 0, \\ -x & \text{für } x < 0. \end{cases}$$

Behauptung: Sei $c > 0$, und weiterhin gelte $|x| < c$ für $x \in \mathbb{R}$. Dann gilt:

$$-c < x < c.$$

Beweis durch Fallunterscheidung:

Fall 1: Sei $x \geq 0$. Dann gilt $x = |x| < c$ und $-c < x$ (da $-c$ negativ ist).

Fall 2: Sei $x < 0$. Dann gilt $x < c$ und $-x = |x| < c$, womit $x > -c$. ■

3.6 Vollständige Induktion

Ziel: Wir wollen Aussagen der Form

$$\forall n \in \mathbb{N} : A(n)$$

beweisen. Dabei ist $A(n)$, für $n \in \mathbb{N}$, eine Aussageform.

Mit anderen Worten: Wir betrachten Aussagen $A(n)$ zu natürlichen Zahlen $n \in \mathbb{N}$, die für alle $n \in \mathbb{N}$ verifizieren wollen.

Beweismethode: Wir verwenden den Beweis der `vollständigen Induktion`.

Ausgangspunkt für unsere Erklärungen ist das `Vollständigkeitsaxiom`, das wir bereits bei der Einführung der natürlichen Zahlen kennengelernt haben. Wir werden gleich an das Vollständigkeitsaxiom erinnern, bevor wir daraus dann die Beweismethode der vollständigen Induktion herleiten.

Herleitung über das Vollständigkeitsaxiom.

Erinnerung: Für $M \subset \mathbb{N}$ gilt das Vollständigkeitsaxiom

$$1 \in M \wedge (\forall n \in M : [n \in M \Longrightarrow (n+1) \in M]) \qquad \Longrightarrow \qquad M = \mathbb{N}.$$

Wir definieren nun die Menge

$$M := \{n \in \mathbb{N} \,|\, A(n)\} \subset \mathbb{N},$$

d.h. wir fassen in M alle $n \in \mathbb{N}$ zusammen, für die die Aussage $A(n)$ wahr ist.

Damit reformulieren wir das Vollständigkeitsaxiom für dieses M wie folgt:

$$A(1) \wedge (\forall n \in M : [A(n) \Longrightarrow A(n+1)]) \qquad \Longrightarrow \qquad M = \mathbb{N}.$$

Fazit: Falls $A(1)$ gilt, und falls für $n \in M$ unter Voraussetzung der Aussage $A(n)$ die Aussage $A(n+1)$ folgt, so gilt $M = \mathbb{N}$, d.h. in diesem Fall gilt

$$\{n \in \mathbb{N} \,|\, A(n)\} = \mathbb{N},$$

so dass die Aussage $A(n)$ für alle $n \in \mathbb{N}$ wahr ist. Genau das wollen wir zeigen!

Konstruktion der vollständigen Induktion.

Wir wollen nun aus den bisherigen Erkenntnissen die Beweistechnik der vollständigen Induktion konstruieren. Dies machen wir schrittweise wie folgt.

- **Induktionsanfang** ($n = 1$): Wir zeigen die Aussage $A(1)$.
- **Induktionsvoraussetzung**: Wir nehmen an, $A(n)$ gelte für $n \in \mathbb{N}$.
- **Induktionsschluss** ($n \to n + 1$):
  Unter der Voraussetzung $A(n)$ zeigen wir $A(n + 1)$.

Fazit: Falls wir die obigen Schritte, insbesondere die Überprüfung von $A(1)$ [im Induktionsanfang - das ist häufig sehr einfach], sowie weiterhin den Schritt von n nach $n + 1$ [im Induktionsschluss - das ist der schwierigste Schritt] fehlerfrei durchführen können, so ist der Nachweis für die Gültigkeit von $A(n)$, für alle $n \in \mathbb{N}$ schließlich erbracht. Damit wäre der Beweis dann komplett.

Wir setzen unsere Diskussion nun mit ausgewählten Beispielen fort.

Einschub: Endliche Summen und Produkte.

Definition: Für $m, n \in \mathbb{Z}$ seien $b_m, \ldots, b_n \in \mathbb{R}$ reelle Zahlen. Dann ist die (endliche) Summe der Summanden $b_m, \ldots, b_n$ definiert durch

$$\sum_{k=m}^{n} b_k := \begin{cases} b_m + b_{m+1} + \ldots + b_n & \text{für } m \leq n, \\ 0 & \text{für } m > n. \end{cases}$$

Für $m > n$ verwenden wir die Bezeichnung leere Summe.

Weiterhin ist das (endliche) Produkt der Faktoren $b_m, \ldots, b_n$ definiert durch

$$\prod_{k=m}^{n} b_k := \begin{cases} b_m \cdot b_{m+1} \cdot \ldots \cdot b_n & \text{für } m \leq n, \\ 1 & \text{für } m > n. \end{cases}$$

Für $m > n$ verwenden wir die Bezeichnung leeres Produkt. ◯

Ein klassisches Beispiel.

Ziel: Wir wollen für $n \in \mathbb{N}$ eine geschlossene Formel für die Summe

$$\sum_{k=1}^{n} k := 1 + 2 + 3 + \ldots + (n-2) + (n-1) + n.$$

entwickeln. Heuristisch erkennen wir nach Umsortieren der Summanden

$$\sum_{k=1}^{n} k = (1+n)+(2+(n-1))+(3+(n-2))+\ldots+\left(\frac{n}{2}+\left(\frac{n}{2}+1\right)\right) = (n+1)\cdot\frac{n}{2}$$

für n *gerade* bzw.

$$\sum_{k=1}^{n} k = (1+n)+(2+(n-1))+\ldots+\left(\frac{n-1}{2}+\frac{n+3}{2}\right)+\frac{n+1}{2} = (n+1)\cdot\frac{n}{2}$$

für n *ungerade*. Damit *vermuten* wir die `Summenformel von Gauß`

$$\sum_{k=1}^{n} k = \frac{(n+1)\cdot n}{2} \qquad \text{für } n \in \mathbb{N}.$$

Beweis der Summenformel von Gauß[a].

Behauptung: Für alle $n \in \mathbb{N}$ gilt die Summenformel

$$\sum_{k=1}^{n} k = \frac{(n+1) \cdot n}{2}.$$

Beweis durch vollständige Induktion:

- *Induktionsanfang*: Für $n = 1$ gilt die Formel mit $\sum_{k=1}^{1} k = 1 = (1+1) \cdot 1/2$.
- *Induktionsvoraussetzung*: Die Formel gelte für $n \in \mathbb{N}$.
- *Induktionsschluss* $(n \to n+1)$: Es gilt

$$\sum_{k=1}^{n+1} k = \sum_{k=1}^{n} k + (n+1) = \frac{(n+1) \cdot n}{2} + (n+1) = \frac{(n+1) \cdot (n+2)}{2},$$

wobei wir beim Übergang des zweiten Gleichheitszeichens die Gültigkeit der Summenformel für n (d.h. die Induktionsvoraussetzung) verwendet haben. ■

[a] Carl Friedrich Gauss (1777-1855), deutscher Mathematiker, Astronom und Physiker

Der Fundamentalsatz der Arithmetik.

Theorem (Fundamentalsatz der Arithmetik): *Jede natürliche Zahl* $n \geq 2$ *lässt sich als Produkt*

$$n = p_1^{r_1} \cdot p_2^{r_2} \cdot \ldots \cdot p_k^{r_k},$$

von Primzahlpotenzen schreiben, mit paarweise verschiedenen Primzahlen $p_j \in \mathbb{P}$ *und mit Exponenten* $r_j \in \mathbb{N}$, *für* $1 \leq j \leq k$.

Beweis: durch Induktion nach n.

- Induktionsanfang ($n = 2$): Es gilt $2 = 2^1$.
- *Induktionsvoraussetzung*: Die Aussage des Theorems gelte für $n \geq 2$.
- *Induktionsschluss* ($n \to n+1$):

Fall 1: Sei $n+1$ eine Primzahl. Dann gilt $n+1 = (n+1)^1$.
Fall 2: Sei $n+1$ *keine* Primzahl. Dann gibt es $k, m \leq n$ mit $n+1 = k \cdot m$.
Somit besitzt $n+1$ eine Primfaktorzerlegung, da k und m je eine besitzen. ■

Bemerkung: Für $n > 1$ sind die (verschiedenen) Basen $p_1, \ldots, p_k$ und die zugehörigen Exponenten $r_1, \ldots, r_k \geq 1$ der Primfaktorzerlegung eindeutig. □

Potenzmengen.

Definition: Für eine Menge M wird die Menge $\mathcal{P}(M) := \{N \mid N \subset M\}$ ihrer Teilmengen als `Potenzmenge` von M bezeichnet. ◯

Bemerkung: Die `leere Menge` $\emptyset$ (diejenige Menge, die kein Element enthält) liegt stets in $\mathcal{P}(M)$, d.h. $\emptyset \in \mathcal{P}(M)$. Somit gilt $\emptyset \in \mathcal{P}(\emptyset)$ für die Potenzmenge von $\emptyset$. Weiterhin ist jede Menge M ein Element von $\mathcal{P}(M)$, d.h. $M \in \mathcal{P}(M)$. □

Wir wollen nun für *endliche* Mengen $M = \{m_1, \ldots, m_n\}$, $n \in \mathbb{N}$, die Anzahl der Elemente in $\mathcal{P}(M)$ bestimmen. Hierzu betrachten wir den Fall *kleiner* $n \in \mathbb{N}_0$.

- $n = 1$: Die Menge $M_1 = \{m_1\}$ besitzt nur die *zwei* Teilmengen $\emptyset, \{m_1\}$.
- $n = 2$: Die Menge $M_2 = \{m_1, m_2\}$ besitzt die *vier* Teilmengen

$$\emptyset, \{m_1\}, \{m_2\}, \{m_1, m_2\}.$$

- $n = 3$: Die Menge $M_3 = \{m_1, m_2, m_3\}$ besitzt *acht* Teilmengen, nämlich die vier Teilmengen von $\mathcal{P}(M_2)$ (siehe $n = 2$), sowie die vier Teilmengen

$$\{m_3\}, \{m_1, m_3\}, \{m_2, m_3\}, \{m_1, m_2, m_3\}.$$

Zur Größe von Potenzmengen.

Nach unseren Überlegungen *vermuten* wir die Gültigkeit des folgenden Satzes, den wir gleich beweisen. Dabei verwenden wir die Notation $M_n = \{m_1, \ldots, m_n\}$ sowie $|M_n| = n$ für die Anzahl der Elemente in M_n, wobei $n \in \mathbb{N}$.

Satz: *Eine n-elementige Menge besitzt 2^n Teilmengen, für $n \in \mathbb{N}$.*

Beweis durch vollständige Induktion nach n:

- Induktionsanfang ($n = 1$): Es gilt $|\mathcal{P}(M_1)| = 2 = 2^1$.
- *Induktionsvoraussetzung*: Die Aussage gelte für $n \in \mathbb{N}$, d.h. $|\mathcal{P}(M_n)| = 2^n$.
- *Induktionsschluss* ($n \to n+1$): Zu zeigen: $|\mathcal{P}(M_{n+1})| = 2^{n+1}$.

Wir verwenden dazu die Zerlegung $\mathcal{P}(M_{n+1}) = K_1 \cup K_2$, wobei

$$T \in K_1 \iff m_{n+1} \notin T \qquad \text{und} \qquad T \in K_2 \iff m_{n+1} \in T,$$

so dass $K_1 \cap K_2 = \emptyset$, d.h. die Mengen $K_1, K_2 \in \mathcal{P}(M_{n+1})$ sind `disjunkt`.

Nach Induktionsvoraussetzung besitzen K_1 und K_2 jeweils genau 2^n Elemente.

Somit besitzt $\mathcal{P}(M_{n+1})$ insgesamt $2^n + 2^n = 2^{n+1}$ Elemente. ■

Anordnungsmöglichkeiten in endlichen Mengen.

Definition: Für $n \in \mathbb{N}$ ist $n!$ (gelesen: n Fakultät) das Produkt

$$n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (n-2) \cdot (n-1) \cdot n.$$

Weiterhin setzen wir $0! := 1$. ○

Satz: *Eine n-elementige Menge $M = \{m_1, \ldots, m_n\}$ besitzt $n!$ verschiedene Anordnungen (Permutationen) ihrer Elemente $m_1, \ldots, m_n \in M$.*

Beweis durch vollständige Induktion nach n:

• *Induktionsanfang* ($n = 1$): Für eine einelementige Menge $M = \{m_1\}$ gibt es nur *eine* Anordnung des Elements m_1. Mit $1! = 1$ gilt die Aussage für $n = 1$.

• *Induktionsvoraussetzung*: Die Behauptung gelte für $n \in \mathbb{N}$.

• *Induktionsschluss* ($n \to n+1$): Die Anzahl der Anordnungen für eine $(n+1)$-elementige Menge $M = \{m_1, \ldots, m_n, m_{n+1}\}$ zerfällt in $n+1$ Klassen: In jeder dieser Klassen ist eines der Elemente m_k, für $1 \leq k \leq n+1$, führend, während es für die übrigen n Elemente aus $M \setminus \{m_k\}$ nach Voraussetzung $n!$ Anordnungen gibt. Somit gibt es $(n+1)! = (n+1) \cdot n!$ Anordnungen in M. ■

Folgerung: *Eine n-elementige Menge $M = \{m_1, \ldots, m_n\}$ besitzt genau*

$$\binom{n}{m} := \frac{n!}{m!(n-m)!}, \qquad \textit{für } n, m \in \mathbb{N}_0 : 0 \leq m \leq n,$$

m-elementige Teilmengen.

Beweis: Es gibt $n!$ Permutationen von $(m_1, \ldots, m_n)$, die wir mit

$$(m_{i_1}, \ldots, m_{i_n}), \qquad \text{für } \{i_1, \ldots, i_n\} = \{1, \ldots, n\},$$

bezeichnen. Betrachte nun die ersten m Einträge in $(m_{i_1}, \ldots, m_{i_n})$. Die $n!$ Permutationen

$$(m_{i_1}, \ldots, m_{i_m}, m_{i_{m+1}}, \ldots, m_{i_n})$$

von $(m_1, \ldots, m_n)$ führen genau $m!(n-m)!$-mal auf die gleiche Teilmenge

$$\{m_{i_1}, \ldots, m_{i_m}\} \subset \{m_1, \ldots, m_n\},$$

denn die $m!$ Permutationen der ersten m Einträge und die $(n-m)!$ Permutationen der restlichen $n-m$ Einträge verändern $\{m_{i_1}, \ldots, m_{i_m}\}$ nicht. Somit gibt es $\frac{n!}{m!(n-m)!} = \binom{n}{m}$ m-elementige Teilmengen von $\{m_1, \ldots, m_n\}$. ■

Binomialkoeffizienten.

Definition: Für nichtnegative ganze Zahlen $n, k \in \mathbb{N}_0$ mit $k \leq n$ wird die Zahl

$$\binom{n}{k} := \frac{n!}{k!(n-k)!}$$

als Binomialkoeffizient (gelesen: n über k) bezeichnet. Weiterhin setzen wir

$$\binom{n}{k} := 0 \qquad \text{falls } k > n \text{ oder } k < 0.$$

○

Bemerkung: Man kann die Binomialkoeffizienten ebenso durch das Produkt

$$\prod_{j=1}^{k} \frac{n-j+1}{j} = \frac{n(n-1)\cdot\ldots\cdot(n-k+1)}{1\cdot 2\cdot\ldots\cdot k}$$

einführen. Diese Darstellung ist jedoch *unpraktisch*. Mehr dazu später. □

Eigenschaften von Binomialkoeffizienten.

Satz: Für Binomialkoeffizienten gelten die folgenden Eigenschaften.

(a) Für $n, k \in \mathbb{N}_0$ gilt die Symmetrie

$$\binom{n}{k} = \binom{n}{n-k}$$

(b) Für $1 \leq k \leq n$ gilt die Rekursion

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}.$$

Beweis: Leichte Übung — einfach die Definition einsetzen und rechnen. □

Der Binomische Lehrsatz.

Ziel: Wir wollen eine Darstellung für $(a+b)^n$ entwickeln, wobei $n \in \mathbb{N}_0$ und $a, b \in \mathbb{R}$. Wir betrachten zunächst *kleine* n. Das *kleinstmögliche* ist hier $n = 0$.

- $n = 0$: $(a+b)^0 = 1$
- $n = 1$: $(a+b)^1 = a+b$
- $n = 2$: $(a+b)^2 = a^2 + 2ab + b^2$
- $n = 3$: $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$.

Satz (Binomischer Lehrsatz): *Für* $n \in \mathbb{N}_0$ *und* $a, b \in \mathbb{R}$ *gilt*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

Vorbemerkung: Wir führen den Beweis durch vollständige Induktion nach n. Dabei ist $n = 0$ das *kleinstmögliche* n, für das die Behauptung des Satzes sinnvoll und korrekt ist. Daher starten wir im Induktionsanfang mit $n = 0$. □

Beweis des binomischen Lehrsatzes.

Satz (Binomischer Lehrsatz): *Für* $n \in \mathbb{N}_0$ *und* $a, b \in \mathbb{R}$ *gilt*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

Beweis durch vollständige Induktion nach n:

- *Induktionsanfang* $(n = 0)$: Es gilt

$$(a+b)^0 = \binom{0}{0} a^0 b^0 = 1.$$

- *Induktionsvoraussetzung*: Die Behauptung gelte für $n \in \mathbb{N}_0$.

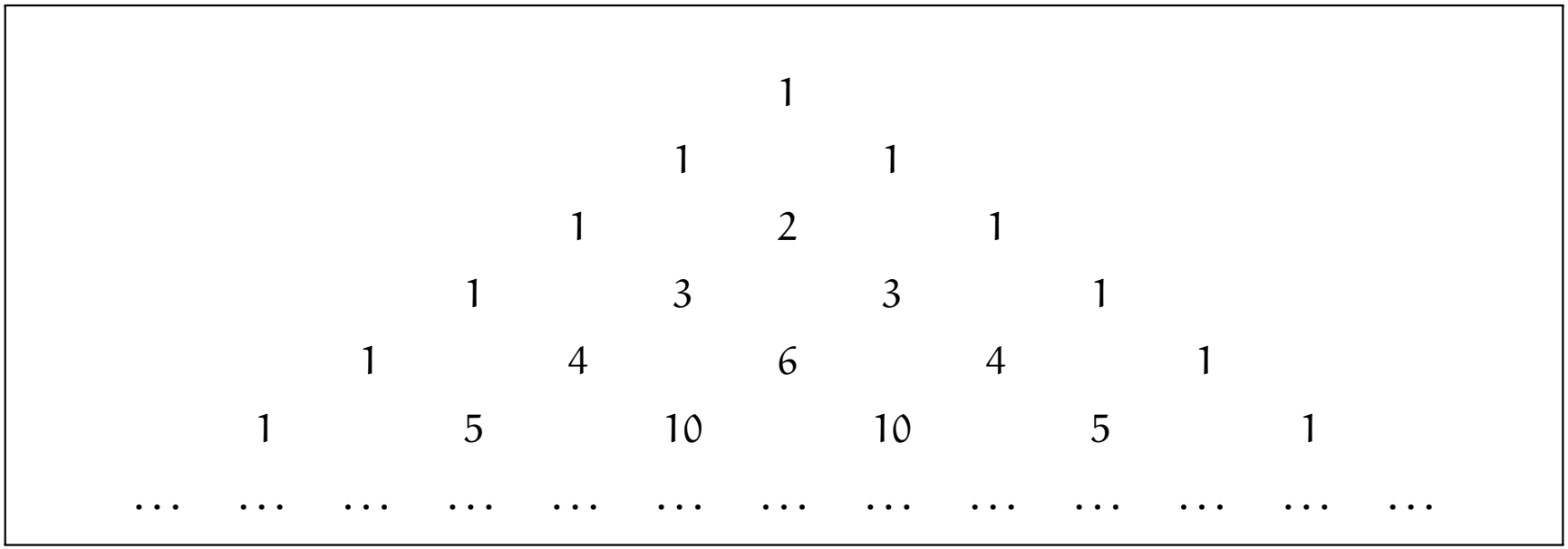
Beweis des binomischen Lehrsatzes (Fortsetzung).

- *Induktionsschluss* $(n \to n+1)$: Es gilt

$$
\begin{aligned}
(a+b)^{n+1} &= (a+b)(a+b)^n = (a+b)\sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k} \\
&= \sum_{k=0}^{n}\binom{n}{k}a^{k+1}b^{n-k} + \sum_{k=0}^{n}\binom{n}{k}a^k b^{n+1-k} \\
&= \sum_{k=1}^{n+1}\binom{n}{k-1}a^k b^{n+1-k} + \sum_{k=0}^{n}\binom{n}{k}a^k b^{n+1-k} \\
&= \binom{n}{0}a^0 b^{n+1} + \sum_{k=1}^{n}\left[\binom{n}{k} + \binom{n}{k-1}\right]a^k b^{n+1-k} + \binom{n}{n}a^{n+1}b^0 \\
&= \binom{n+1}{0}a^0 b^{n+1} + \sum_{k=1}^{n}\binom{n+1}{k}a^k b^{n+1-k} + \binom{n+1}{n+1}a^{n+1}b^0 \\
&= \sum_{k=0}^{n+1}\binom{n+1}{k}a^k b^{n+1-k}
\end{aligned}
$$

■

Rekursive Berechnung der Binomialkoeffizienten.



Das Pascalsche[a] Dreieck.

Ausgangspunkt: Die *Rekursion* $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$.

Beispiel: Für $n = 5$ bekommen wir die binomische Formel

$$(a+b)^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5.$$

[a] Blaise Pascal (1623-1662), französischer Mathematiker, Physiker, Literat, Philosoph